IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

EMANUYEL AMINOV, Individually and on Behalf of All Others Similarly Situated,	*	
Plaintiff,	*	
vs.	*	Civil Action No. _____
CAPITAL ONE FINANCIAL CORPORATION, CAPITAL ONE BANK (USA), N.A., AND CAPITAL ONE, N.A.	*	JURY TRIAL DEMANDED
	*	INJUNCTIVE RELIEF DEMANDED
Defendants.	*	
	*	

CLASS ACTION COMPLAINT

Plaintiff Emanuyel Aminov ("Plaintiff" or "Aminov"), individually and on behalf of all others similarly situated, upon personal knowledge of the facts pertaining to him and on information and belief as to all other matters, and upon the investigation conducted by Plaintiff's counsel, brings this class action complaint against Capital One Financial Corporation, Capital One Bank (USA), N.A., and Capital One, N.A. ("Capital One" or "Defendants"), and alleges as follows:

NATURE OF THE ACTION

1. This action arises from one of the largest bank data security breaches in U.S. history. On July 29, 2019, Capital One announced that an unauthorized party had gained access to one of its cloud-based servers (the "Server"), used to store private and identifying information about its customers, including information customers were required to and did provide when applying for Capital One products and services and data maintained by the company that tracked

its customers' activities (collectively, "Personal Information").[1] According to a criminal complaint filed that same day in the federal district court in Seattle, the unauthorized party – identified as Paige Thompson – is alleged to have repeatedly accessed or attempted to access the Server with impunity for over a four month period and copied the Personal Information of ***106 million*** Capital One customers into her own private storage site (the "Data Breach" or "Breach").[2]

2. Capital One's announcement revealed that the unauthorized access to its Server began in March 2019 and continued unabated until July 2019, giving criminals ample opportunity to access and download Plaintiffs' Personal Information for months. In the criminal complaint, prosecutors explained that Thompson – a former employee of Amazon Web Services, which hosted the breached Server – exploited a negligently configured firewall on Capital One's system in order to access customers' data on the Capital One Server at various times between March 12 and July 17, 2019.

3. According to Capital One, the Breach was only discovered after an anonymous "ethical" or "white hat" hacker notified the company in July 2019 that its customers' data appeared to be leaked online (*i.e.*, made available for anyone to obtain and use for nefarious purposes).

4. The scope of the Data Breach cannot be understated: there are ***106 million*** known victims, thus far, of Capital One's security failures, and investigations are ongoing.

---

[1] Capital One Newsroom, *Capital One Announces Security Incident*, Capital One (July 29, 2019), press.capitalone.com/phoenix.zhtml?c=251626&p=irol-newsArticle_pf&ID=2405043; *Frequently Asked Questions*, Capital One (last updated July 31, 2019), https://www.capitalone.com/facts2019/ (collectively hereinafter, "Breach Notification").

[2] Complaint for Violation of 18 U.S.C. 1030(a)(2), ECF No. 1, *United States of America v. Paige A. Thompson, a/k/a "erratic"*, Case No. 2:19-mj-00344-MAT (W.D. Wa.) (hereinafter, "Thompson Complaint").

5. Although Capital One's July 29, 2019 announcement states, without providing evidence, that it does not believe it is likely its customers' data has been disseminated or used to commit identity fraud,[3] the hacker herself unequivocally stated her intent to distribute the data at least a month prior to being discovered.[4]

6. As the result of Capital One's failure to reasonably secure its Server, a cybercriminal with a stated intent to distribute obtained the Personal Information of over 100 million customers, including Plaintiff and the other Class members, exposing them to an increased risk of fraud and identity theft, and causing them injuries and damages, including, but not limited to, the lost value of their Personal Information, and the lost time and expense necessary to protect themselves against the foreseeable fraud and identity theft that Capital One's conduct caused. Plaintiff and Class members are further damaged as their Personal Information remains in Capital One's possession, without adequate protection.

JURISDICTION AND VENUE

7. This Court has jurisdiction under 28 U.S.C. §1332(a)(1) as modified by the Class Action Fairness Act of 2005, because Plaintiff and Defendants are citizens of different states, there are more than 100 members of the class, and the aggregate amount in controversy exceeds $5,000,000.00, exclusive of attorneys' fees, interest, and costs.

8. Venue is proper in this District under 28 U.S.C. §1391 because Defendants engaged in substantial conduct relevant to Plaintiff's claims within this District and are headquartered and have their principal place of business in this District.

---

[3] Breach Notification.

[4] Thompson Complaint, at ¶25.

PARTIES

9. Plaintiff Emanuyel Aminov resides in and is a citizen of the State of New York. Between 2005 and 2019, Plaintiff applied for and obtained three credit cards through Capital One. When opening his accounts, Plaintiff provided Capital One with certain Personal Information. In doing so, Plaintiff believed that Capital One took all reasonable, necessary, legally required, and industry standard security measures to protect the Personal Information he provided and the Personal Information contained within his accounts (*i.e.*, transaction and payment histories, credit limits, and balances), and that his Personal Information would remain private. As a result of Capital One's failure to protect his Personal Information, Plaintiff suffered injuries and damages, including, but not limited to, loss in value of his Personal Information, an increased risk of identity theft, and loss of time and money spent to protect himself from the foreseeable risk of fraud and identify theft.

10. Capital One Financial Corporation ("Capital One Financial") is a Delaware corporation with its principle place of business at 1680 Capital One Drive, McLean, VA 22102. Capital One Financial offers a broad array of financial products and services to consumers, small business, and commercial clients, including banking and credit cards. Capital One Financial operates through two primary subsidiaries: Capital One Bank (USA), N.A. and Capital One, N.A.

11. Capital One Bank (USA), N.A. ("Capital One Bank") is a national association and operating subsidiary of Capital One Financial with its principle place of business at 4851 Cox Road, Glen Allen, VA 23060. Capital One Bank operates as a bank and serves consumers, small businesses, and commercial clients worldwide, offering checking accounts, credit and debit cards, loans, insurance, payment protection, phone banking, bill pay, lending, and online banking services.

12. Capital One, N.A. is a is a national association and operating subsidiary of Capital One Financial with its principal place of business at 1680 Capital One Drive, McLean, VA 22102. It offers banking products and services to small business and commercial clients.

13. Capital One Financial, Capital One Bank, and Capital One, N.A. are collectively referred to herein as "Capital One."

SUBSTANTIVE ALLEGATIONS COMMON TO ALL COUNTS

A. Capital One's Commitment to Security and Privacy Protections

14. Capital One is a global financial services that began in 1994. In 25 years, it has grown to become a Fortune 500 company traded on the New York Stock Exchange under the symbol "COF" and included in the S&P 100 index.

15. Capital One offers a broad spectrum of financial products and services to consumers, small businesses, and commercial clients through a variety of channels. It supports its services by renting or contracting for computer servers through a cloud-based computing company. Capital One stores customers' Personal Information on these servers, including credit card applications and other information regarding customers and support services.[5]

16. Capital One is now one of the largest banks in the United States – the eighth largest by deposits – with $249.8 billion in deposits and $372.5 billion in total assets as of December 31, 2018.[6] Capital One is also the third largest credit card issuer, the third largest issuer of small

[5] Thompson Complaint, at ¶7.

[6] *Capital One Press Room, Our Company,* Capital One, http://press.capitalone.com/phoenix.zhtml?c=251626&p=irol-factsheet (last visited Aug. 1, 2019).

business credit cards in the U.S., the largest U.S. direct bank, and the second largest financial institution auto loan originator.[7]

17. When customers apply for financial products and services, including credit cards, Capital One requires them to provide Personal Information. Upon information and belief, Capital One stores that information on its servers. It also collects and stores additional Personal Information about its customers, such as payment and transaction history, balances, credit limits, and credit scores.

18. Capital One represents to its customers that it will secure the Personal Information and protect its customers' privacy. It states, "Safeguards are in place to protect your information," and in its technology guarantee, it commits: "We build information security into our systems and networks using internationally recognized security standards, regulations, and industry-based best practices."[8]

19. The Capital One privacy and opt out notice, last updated July 2017, reiterates: "To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."[9]

20. In a Frequently Asked Questions section of its website, Capital One provides the following response to the question, "How does Capital One protect my personal and business information?":

---

[7] *Id*.

[8] *Commitment*, Capital One, https://www.capitalone.com/applications/identityprotection/commitment/ (last visited Aug. 1, 2019) (hereinafter, "*Commitment*").

[9] *Privacy Notice*, Capital One, https://www.capitalone.com/privacy/notice/en-us/ (last visited Aug. 1, 2019).

"We're committed to maintaining the privacy and security of your information so you can feel safe banking no matter where you are.

- We build security into all of our systems and networks.
- Our experts perform internal and external tests on all our applications and systems to safeguard your information.
- We leverage multiple preventative and detective methods to mitigate risks and protect access to your information through a layered security program."[10]

21. In particular, Capital One represents that it protects its customers' Social Security numbers, "collected through any channel or retained in any way by Capital One in connection with customer, employee or other relationships" and states:

"Our policies and procedures:

1. Protect the confidentiality of Social Security numbers;
2. Prohibit the unlawful disclosure of Social Security numbers; and
3. Limit access to Social Security numbers to employees or others with legitimate business purposes."[11]

22. Capital One's representations regarding its data security efforts and privacy protections were false, misleading, and deceptive.

B. Capital One and the Financial Services Industry Were on Notice of a Heightened Data Breach Risk

23. Prior to Capital One's July 29, 2019 Data Breach announcement, numerous articles identified the heightened risk of data breaches faced by the financial services industry.

---

[10] *Commitment*.

[11] *Social Security Number Protections*, Capital One, https://www.capitalone.com/identity-protection/privacy/social-security-number (last visited Aug. 1, 2019).

24. For example, an August 28, 2018 article in Forbes reported:

> The risk of cyberattack on financial services firms cannot be overstated. Cyberattacks cost financial services firms more to address than firms in any other industry at $18 million per firm (vs. $12 million for firms across industries). Financial services firms also fall victim to cybersecurity attacks 300 times more frequently than businesses in other industries. In other words, while the typical American business is attacked 4 million times per year, the typical American financial services firm is attacked a staggering 1 billion times per year.[12]

25. That same article reports that the "rate of breaches, or theft of sensitive data, in the financial services industry has tripled over the past five years."[13]

26. Major banks have acknowledged the serious, impending risk of a security breach. Jamie Dimon, CEO of JPMorgan Chase, has stated that his bank spends almost $600 million a year on security, and Bank of America's CEO has stated in the past that the bank has a "blank check" for cybersecurity.[14]

27. In fact, Capital One itself has faced security breaches in the recent past. In a breach in 2017, "Capital One notified customers that a former employee may have had access for nearly four months to their personal data, including account numbers, telephone numbers, transaction history and Social Security numbers."[15]

---

[12] Bhakti Mirchandani, *Laughing All the Way to the Bank: Cybercriminals Targeting U.S. Financial Institutions,* FORBES (Aug. 28, 2018), https://www.forbes.com/sites/bhaktimirchandani/2018/08/28/laughing-all-the-way-to-the-bank-cybercriminals-targeting-us-financial-institutions/#15f32e796e90.

[13] *Id.*

[14] Emily Flitter and Karen Weise, *Capital One Data Breach Compromises Data of Over 100 Million*, THE NEW YORK TIMES (July 29, 2019), https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html (hereinafter, "*Data Breach Compromises Data*").

[15] *Data Breach Compromises Data.*

28. Capital One reported a similar breach in 2014.[16]

29. In 2017, Capital One CEO and Chairman Richard Fairbank warned investors that a breach the size of the Equifax breach would be very expensive for the company. He stated, "These are bad things for card companies because, every time there's been a breach, I've said to our folks, 'How come card companies end up paying for this and why not the one who did the breach?'"[17]

30. Clearly, Capital One did not heed its own warning. Despite such public information and its own history of breaches putting Capital One on notice of the heightened risk of data breaches faced by the financial services industry, Capital One failed to take adequate steps to protect its customers' Personal Information.

C. Capital One's Recent, Dubious Security Measures

31. According to Bloomberg, some "financial industry executives have cautioned that sensitive consumer data could be put at risk on the cloud. Bank of America Corp., the second-largest U.S. bank, has been reticent to use the public cloud."[18]

32. Despite these cautions, Capital One has pushed forward with its cloud-based security and applications. In April 2019, Fairbank told investors, "We are now considered one of the most cloud-forward companies in the world."[19] According to a Bloomberg article, Fairbank

---

[16] *Id.*

[17] Jennifer Surane and Lananh Nguyen, *Capital One Touted the Cloud's Safety as Hacker Was Breaching It*, BLOOMBERG (July 30, 2019), https://www.bloomberg.com/news/articles/2019-07-30/capital-one-touted-the-cloud-s-safety-as-hacker-was-breaching-it (hereinafter, "*Touted the Cloud's Safety*").

[18] *Touted the Cloud's Safety.*

[19] *Id.*

has been "one of the financial industry's most vocal proponents for shifting sensitive customer information to outside cloud services."[20]

33. In recent years, Capital One hired thousands of engineers and developed its application programming interface to share data more seamlessly through the cloud.[21] In particular, Capital One selected Amazon Web Services for its cloud-based security model and has committed to moving all of its customer data to the cloud by the end of 2020.[22]

D. The Data Breach

34. On July 29, 2019, Capital One announced that a hacker had broken through its negligently misconfigured firewall and accessed and copied 106 million customers' Personal Information from the company's cloud-based Server.[23]

35. It is not clear, based on publicly available information or through statements made by Capital One, when Capital One first became aware of the Breach, but Capital One claims that it was first alerted to the possibility of a Data Breach on July 17, 2019. On that date, an ethical hacker, not related to or employed by Capital One, sent an email to an email address that Capital One maintains in order to solicit disclosures of actual or potential vulnerabilities in its computer

---

[20] *Id.*

[21] *Id.*; *see also "How to Cloud" with Capital One: How Capital One Reduced its Data-Center Footprint, Expanded its Use of Microservices, and Reimagined Banking Using AWS*, AWS, https://aws.amazon.com/solutions/case-studies/capital-one-enterprise/ (last visited Aug. 1, 2019).

[22] Peter Cohan, *Will Capital One's 106M Name Data Breach Cut Into AWS's Growth?*, FORBES (July 30, 2019), https://www.forbes.com/sites/petercohan/2019/07/30/will-capital-ones-106m-name-data-breach-cut-into-awss-growth/#18f5b1e49d51.

[23] Breach Notification.

systems. The email warned that there appeared to be leaked data belonging to Capital One's customers on GitHub.com.[24]

36. Capital One then proceeded to investigate the claim; it examined the GitHub file, which was timestamped April 21, 2019, and determined that the file contained the IP address for a specific Capital One server. Capital One further determined that a "firewall misconfiguration permitted commands to reach and be executed by that server, which enabled access to folders or buckets of data" in the cloud-based Server.[25]

37. The April 21st file contained code for three commands, as well as a list of more than 700 folders or buckets of data.[26] Capital One tested the three commands and confirmed that they did indeed give outsiders the ability "to obtain Capital One's credentials, to list or enumerate folders or buckets of data, and to extract data from certain of those folders or buckets."[27] In particular, "Capital One confirmed that the more-than-700 folders or buckets of data listed in the April 21 File matched the actual names of folders or buckets of data used by Capital One for data stored" on the Server.[28]

38. Further, according to the Thompson Complaint, Capital One's logs show a number of connections or attempted connections using those commands from masked IP addresses, all with the same beginning numbers, which Capital One believes to be related to activity conducted

---

[24] Thompson Complaint, at ¶¶8-9.

[25] *Id.* at ¶10.

[26] *Id.* at ¶11.

[27] *Id.* at ¶12.

[28] *Id.*

by the same person involved in the April 21, 2019 intrusion. Each log entry shows "similar unusual miscommunications through the misconfigured firewall to the" Server.[29]

39. The FBI's investigation into the Breach identified Thompson as the architect of the intrusion. Thompson's posts on several websites and social media sites strongly suggest that she intended to sell or distribute the Personal Information. For instance, on June 18, 2019, Thompson appears to have posted on Twitter:

> "Ive basically strapped myself with a bomb vest, fucking dropping capitol ones dox and admitting it"
>
> "I wanna distribute those buckets i think first"
>
> "There ssns…with full name and dob"[30]

40. The FBI Special Agent investigating Thompson understood this post to indicate that Thompson "intended to disseminate data stolen from victim identifies, starting with Capital One."[31]

41. The Personal Information that was stolen as a result of Capital One's failures includes its customers' most sensitive information: credit scores, limits, balances, and payment history; contact information, inducing ZIP codes and email addresses; dates of birth; self-reported income and payments history; fragments of transaction data during 2016, 2017, and 2018; 140,000 Social Security numbers of credit card customers; and 80,000 linked bank-account numbers from secured credit-card customers. This is extraordinarily intimate data that includes rarer prizes for hackers, such as dates of birth, social security, and bank account numbers.

---

[29] *Id.* at ¶13.

[30] *Id.* at ¶25.

[31] *Id.*

42. In total, 100 million U.S. customers' Personal Information was taken, and likely even more exposed. Another 6 million customers in Canada were affected. Most at risk are consumers and small businesses who applied for credit card products through Capital One between 2005 and early 2019 because, the data copied includes primarily data related to credit card applications, some of which is not tokenized or encrypted.[32]

E. Capital One Failed to Implement Basic Security Measures that Would Have Prevented the Data Breach

43. On information and belief, Capital One failed to implement reasonable, industry-standard, or appropriate security measures and knowingly, recklessly, or negligently left its customers' Personal Information, including that of Plaintiff and the other Class members, inadequately protected and vulnerable to one of the largest cyber-attacks and data thefts in U.S. history.

44. On information and belief, among Capital One's failures in this respect included its failure to establish adequate firewalls to handle a server intrusion contingency and failure to detect and provide prompt and adequate warnings of security breaches.

45. The investigations into Capital One's failures have only just begun. The Federal Bureau of Investigation is continuing to investigate the Data Breach. Further, Attorney General of New York Letitia James pledged to investigate Capital One's breach and the safeguards missing in Capital One's system that lead to a hack of 100 million U.S. consumers: "It is becoming far too commonplace that financial institutions are susceptible to hacks, begging the questions: Why do

[32] *Id.* at ¶14.

these breaches continue to take place? And are companies doing enough to prevent future data breaches?"[33]

F. Capital One Knew or Should Have Known That the Server Was Vulnerable to Attack

46. Capital One knew or should have known that its below industry-standard security systems and unreasonably vulnerable technologies would render the Server an aim of attack by third-parties.

47. Despite the ever-existing threat of a security breach, particularly ones targeting the financial services industry, and despite Capital One's actual knowledge of the vulnerabilities of its computer systems from prior data breaches, Capital One recklessly, negligently, and unreasonably failed to implement adequate safeguards to protect the Sever, and failed to take steps to protect Plaintiff's and the other Class members' Personal Information stored on the Server.

G. The Importance of Protecting Personal Information

48. Consumers have a vested interest in protecting all of their confidential or private information, ranging from their addresses, dates of birth, bank account information, credit card information, debit card information, social security numbers, asset information, employment information and other Personal Information.

49. The significant impact identity theft can have on consumers, and the extreme financial ramification the failure to secure personal information can cause, has led to the enactment of numerous privacy-related laws aimed at protecting consumer information and requiring timely disclosures of any breach, including, for example: (1) Virginia Personal Information Protection

[33] Quentin Fottrell, *Everything you wanted to know about hacks and data breaches, but were afraid to ask*, MARKETWATCH (Aug. 1, 2019), https://www.marketwatch.com/story/100-million-capital-one-customers-were-hacked-everything-you-need-to-know-about-data-breaches-but-are-afraid-to-ask-2019-07-30 (Hereinafter, "*Afraid to Ask*").

Act, Va. Civ. Code §59.1-442, *et seq.*; (2) the Virginia Data Breach Notification Law, Va. Criminal Code §18.2, *et seq.*; (2) Gramm-Leach-Bliley Act; (3) Fair Credit Reporting Act; (4) Fair and Accurate Credit Transactions Act; (5) Federal Trade Commission Act, 15 U.S.C. §§41-58; (6) Driver's Privacy Protection Act; (7) HIPPA; (8) The Privacy Act of 1974; (9) Social Security Act Amendments of 1990; (10) E-Government Act of 2002; and (11) Federal Information Security Management Act of 2002.

50. Protection of consumers' private information is obviously critical. Capital One has openly acknowledged, "Safeguarding our customers' information is essential to our mission and our role as a financial institution."[34]

51. Capital One's July 29, 2019 announcement also included a clear acknowledgment by the company's CEO that the breach of its customers' Personal Information was cause for fear and concern: "I am deeply sorry for what has happened . . . I sincerely apologize for the understandable worry this incident must be causing those affected[.]"[35]

52. Consumers are at the mercy of the security measures or controls utilized by those entities that use or maintain their confidential or private information. Consumers, likewise, have no ability to ascertain whether their private information is being adequately protected or, worse, if their private information has been compromised, in any way. Where, as here, Personal Information is and has been inadequately protected, and the entity maintaining that information conceals the inadequate safety measures and the possibility that a breach occurred or is occurring, consumers

---

[34] Breach Notification.

[35] Breach Notification; *see also* Christian Berthelsen, Matt Day, and William Turton, *Capital One Says Breach Hit 100 Million Individuals in U.S.,* BLOOMBERG (July 29, 2019), https://www.bloomberg.com/news/articles/2019-07-29/capital-one-data-systems-breached-by-seattle-woman-u-s-says?srnd=cybersecurity.

become highly vulnerable to identity theft and are hamstrung in their ability to timely react to protect themselves from identity theft following a data breach.

H. Capital One's Failures Have Harmed Plaintiff and the Other Class Members

53. As a result of the Data Breach, Plaintiff and the Other Class members were deprived of the value in their Personal Information and now face an increased risk of identity theft identity theft, and the constant fear, anxiety, and hardship that comes with it, as well as lost time and money required to take steps to protect themselves from identity theft.

54. Indeed, Personal Information is a valuable commodity. A "cyber black-market" exists in which criminals openly sell and trade stolen credit card numbers and other personally identifiable information on a number of Internet websites, including on the heavily encrypted "Dark Web," which is difficult for authorities to monitor.

55. The minimally necessary steps to mitigate (but not eliminate) the threat of identity theft faced by Plaintiff and the Class members are time-consuming and burdensome. Plaintiff and the Class members will be forced to replace their credit and debit cards and to update their payment information on all automatic payment accounts, and victims must add themselves to credit fraud watch lists, which substantially impairs their ability to obtain additional credit. Immediate notice of the Data Breach (which Capital One failed to provide) was essential to obtain the best protection afforded by these services.

56. Capital One claims that is providing its impacted customers with two years of free credit monitoring. But two years of monitoring – without any insurance against identity theft – is woefully insufficient to protect Plaintiff and the Class members from the harm Capital One caused because Personal Information can exist on the Dark Web for years before it is used to steal a person's identity. Exposure of data that cannot be changed, such as Social Security numbers, are

"the hallmarks of particularly severe data breaches."[36] Credit monitoring only looks for changes on a credit report, that indicates an unauthorized user is attempting to open accounts using an identity fraud victim's Personal Information, but it does not, for instance, prevent someone from taking out a loan in the victim's name.[37]

57. Moreover, while Capital One vaguely promised to learn from its mistakes, it has notably not committed to concretely changing its security practices or investing more into its security infrastructure and breach detection systems, leaving its customers open to future attacks. It stated in its July 29, 2019 press release: "Beyond the adjusting item in 2019, we expect any incremental investments in cybersecurity to be funded within our current budget."[38]

I. Impact of the Breach of Plaintiff

58. Plaintiff maintains three Capital One credit cards, including two Spark® Visa Signature business accounts and a Visa Signature personal account.

59. Plaintiff opened each of these accounts between 2005 and 2019. When doing so, he was required to and did provide Capital One with his Personal Information, including his name, mailing address, phone number, email address, date of birth, gender, social security number, and salary history.

60. Plaintiff believed that Capital One took all reasonable, necessary, legally required, and industry standard security measures to protect his Personal Information, and that his Personal Information would remain private. Plaintiff would not have provided Capital One with his Personal Information, nor would he have signed up for any Capital One credit card accounts and

---

[36] *Afraid to Ask*.

[37] *Id.*

[38] Breach Notification.

paid the fees associated therewith, had he known that Capital One's data security measures were inadequate to protect that information.

61. As a result of Capital One's failure to protect his Personal Information, Plaintiff suffered injuries and damages, including, but not limited to, loss in value of his Personal Information, an increased risk of identity theft, and loss of time and money spent to protect himself from the foreseeable risk of fraud and identify theft.

CLASS ACTION ALLEGATIONS

62. Plaintiff brings this class action under Federal Rules of Civil Procedure 23(a), 23(b)(2), 23(b)(3), and/or 23(c)(4), on behalf of himself and all others similarly situated as members of the following class:

> **All persons in the United States who provided personal information to Capital One and whose personal information was compromised or accessed as a result of the data breach first disclosed by Capital One on July 29, 2019 (the "Class").**

63. Subject to additional information obtained through further investigation and discovery, the foregoing definition of the Class may be expanded or narrowed by amendment or amended complaint. Specifically excluded from the proposed Class are the Defendants, their officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint venturers, or entities controlled by the Defendants, and their heirs, successors, assigns, or other persons or entities related to or affiliated with the Defendants and/or their officers and/or directors, or any of them; the Judge assigned to this action, and any member of the Judge's immediate family.

64. ***Numerosity.*** The members of the Class are so numerous that their individual joinder is impracticable. Plaintiff is informed and believes, and on that basis alleges, that the proposed Class contain many millions of members. The precise number of Class members is unknown to Plaintiff. The true number of Class members is known by the Defendants, however,

and thus, class members may be notified of the pendency of this action by first class mail, electronic mail, and/or by published notice.

65. ***Existence and Predominance of Common Questions of Law and Fact.*** Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting only individual Class members. These common legal and factual questions include, but are not limited to, the following:

(a) whether Capital One engaged in the wrongful conduct alleged herein;

(b) whether Capital One owed a legal duty to Plaintiff and the other Class members to exercise due care in collecting, storing, and safeguarding their Personal Information;

(c) whether Capital One negligently or recklessly breached legal duties owed to Plaintiff and the other Class members to exercise due care in collecting, storing, and safeguarding their Personal Information;

(d) whether Capital One failed to implement and maintain reasonable securities practices and procedures to protect against the Data Breach;

(e) whether Capital One's conduct was negligent or willful;

(f) whether Capital One was unreasonable in its delay of notifying affected customers of the Data Breach;

(g) whether Plaintiff and the other Class members are entitled to actual, statutory, punitive, or other forms of damages, and other monetary relief; and

(h) whether Plaintiff and the other Class members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

66. ***Typicality.*** Plaintiff's claims are typical of the claims of the other Class members because, among other things, Plaintiff and the other Class members were injured through the

substantially uniform misconduct described above. Plaintiff herein is advancing the same claims and legal theories on behalf of himself and all other Class members, and there are no defenses available to Capital One that are unique to Plaintiff.

67. ***Adequacy of Representation.*** Plaintiff will fairly and adequately protect the interests of the members of the Class. Plaintiff has retained counsel highly experienced in complex consumer class action litigation, and Plaintiff intends to prosecute this action vigorously. Plaintiff has no adverse or antagonistic interests to those of the Class.

68. ***Superiority.*** A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members is outweighed by the burden and expense that would be entailed by individual litigation of their claims against Defendants. It would thus be virtually impossible for the Class, on an individual basis, to obtain effective redress for the wrongs done to them. Furthermore, even if Class members could afford such individualized litigation, the court system could not. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts. Individualized litigation would also increase the delay and expense to all parties and the court system from the issues raised by this action. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, economies of scale, and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances here.

69. In addition, the Class may be also certified because:

(a) the prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudication with respect to individual Class members that would establish incompatible standards of conduct for the Defendants;

(b) the prosecution of separate actions by individual Class members would create a risk of adjudications with respect to them that would, as a practical matter, be dispositive of the interests of other Class members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; and/or

(c) Defendants have acted or refused to act on grounds generally applicable to the Class thereby making appropriate final declaratory and/or injunctive relief with respect to the members of the Class as a whole.

70. In the alternative, certain issues presented in this action are suitable for certification under Fed. R. Civ. P. 23(c)(4).

COUNT I

Negligence
On Behalf of the Class

71. Plaintiff repeats, realleges, and incorporates by reference the allegations contained above, as though fully stated herein.

72. Capital One owed a duty to Plaintiff and the other Class members to exercise reasonable care in safeguarding and protecting their Personal Information in its possession from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Capital One's security systems to ensure that Plaintiff's and the other Class members' Personal Information in Capital One's possession was adequately secured and protected. Capital One further had a duty to implement processes that would detect a breach of its security system in a timely manner.

73. Capital One also had a duty to timely discover and disclose to Plaintiff and the other Class members that their Personal Information had been, or was reasonably believed to have been, compromised. Timely discovery and disclosure was necessary so that, among other things,

Plaintiff and the other Class members could take appropriate measures to avoid unauthorized charges to their credit/debit card accounts, monitor their account information and credit reports for fraudulent activity, and freeze their accounts and credit reports as needed.

74. Capital One breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class members' Personal Information in its possession by failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and the other Class members' Personal Information; failing to adequately monitor the security of the Server; allowing unauthorized access to Plaintiff's and the other Class members' Personal Information stored on the Server; and failing to recognize in a timely manner that the Server had been breached.

75. Capital One breached its duty to timely disclose that Plaintiff's and the other Class members' Personal Information in its possession had been, or was reasonably believed to have been, stolen or compromised.

76. But for Capital One's wrongful and negligent breach of its duties owed to Plaintiff and the other Class members, their Personal Information would not have been compromised, and they would not have suffered the injury and damages alleged herein.

77. The injury and harm suffered by Plaintiff and the other Class members was the reasonably foreseeable result of Capital One's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class members' Personal Information within its possession. Capital One knew or should have known that its systems and technologies for processing and securing Plaintiff's and the other Class members' Personal Information had security vulnerabilities.

78. As a result of Capital One's negligence, Plaintiff and the other Class members incurred economic damages relating to expenses for credit monitoring and loss of use of their credit, debit, or bank cards.

COUNT II

Unjust Enrichment
On Behalf of the Class

79. Plaintiff repeats, realleges, and incorporates by reference the allegations contained above, as though fully stated herein.

80. Plaintiff and the other Class members conferred benefits on Capital One by paying for products and services, including interest rates on credit cards, security payments for secured cards, and annual credit cards fees.

81. Capital One knowingly and willingly accepted monetary benefits paid for the goods and services by Plaintiff and the other Class members, but failed to honor its obligations to them, including the protection of their Personal Information.

82. Under the circumstances described herein, it is inequitable for Capital One to retain the monetary benefits at the expense of Plaintiff and the other Class members.

83. By engaging in the conduct described above, Capital One has been unjustly enriched at the expense of Plaintiff and the other Class members. Under the circumstances, it would be contrary to equity and good conscience to permit Capital One to retain the ill-gotten benefits that Capital One received in light of the violations of law detailed herein.

84. As a result of Capital One's unjust enrichment, Plaintiff and the other Class members have suffered injury and are entitled to reimbursement, restitution, and disgorgement by Capital One of the benefit conferred by Plaintiff and the other Class members.

COUNT III

Breach of Implied Contract
On Behalf of the Class

85. Plaintiff repeats, realleges, and incorporates by reference the allegations contained above, as though fully stated herein.

86. The Personal Information of Plaintiff and the Class members was provided to Capital One in exchange for goods and services provided by Capital One. Explicit and implicit in this transaction was a covenant for Capital One to undertake reasonable efforts to safeguard, protect, and secure this information. Also implicit in this transaction was a covenant for Capital One to promptly notify its customers in the event that this information was compromised or at risk.

87. Capital One's recognition of these covenants and obligations is implicit in its representations to Plaintiff and the Class regarding the importance of maintaining security measures to protect Personal Information.

88. This implied contract required Capital One to safeguard the Personal Information of Plaintiff and the Class and prevent that information from being compromised and/or stolen.

89. Capital One did not safeguard and protect the private and confidential information of Plaintiff and the Class and failed to adequately prevent that information from being compromised or available for unauthorized dissemination. To the contrary, Capital One allowed this information to be disclosed to unauthorized parties.

90. As a result, Capital One breached its implied contract with Plaintiff and the Class, thereby causing injury to Plaintiff and the Class.

COUNT IV

Bailment
On Behalf of the Class

91. Plaintiff repeats, realleges, and incorporates by reference the allegations contained above, as though fully stated herein.

92. Plaintiff and the other Class members delivered and entrusted their Personal Information to Capital One for the sole purpose of obtaining certain accommodations.

93. During the time of bailment, Capital One owed Plaintiff and the other Class members a duty to safeguard their Personal Information stored on the Server by maintaining reasonable security procedures and practices to protect such information. As alleged herein, Capital One breached this duty.

94. As a result of Capital One's breach of this duty, Plaintiff and the other Class members have been harmed as alleged herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other Class members, respectfully request that this Court enter an Order:

A. Certifying the Class under Federal Rule of Civil Procedure 23(a), 23(b)(2), and 23(b)(3), appointing Plaintiff as Class Representative, and appointing his undersigned counsel as Class Counsel;

B. For an award of equitable, injunctive and declaratory relief described herein, including judicial supervision of Defendants and a judicial determination of the rights and responsibilities of the parties regarding the remains that are the subject to this action;

C. Finding that Capital One's conduct was negligent, deceptive, unfair, and unlawful as alleged herein;

D. Enjoining Capital One from engaging in the negligent, deceptive, unfair, and unlawful business practices alleged herein;

E. Awarding Plaintiff and the other Class members actual, compensatory, and consequential damages;

F. Awarding Plaintiff and the other Class members statutory damages;

G. Awarding Plaintiff and the other Class members punitive damages;

H. Awarding Plaintiff and the other Class members restitution and disgorgement;

I. Requiring Capital One to provide appropriate credit monitoring services to Plaintiff and the other Class members;

J. Awarding pre-judgment and post-judgment interest;

K. Awarding reasonable attorneys' fees and costs, including expert witness fees; and

L. Granting such other relief as the Court deems just and proper.

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

DATED: August 1, 2019

SILVERMAN THOMPSON SLUTKIN & WHITE LLC

/s/

JODIE E. BUCHMAN (VSB NO. 91929)
jbuchman@mdattorney.com
PIERCE C. MURPHY (VSB No. 87842)
pmurphy@mdattorney.com
201 N. Charles Street, 26th Floor
Baltimore, Maryland 21201
Telephone: 410/385-2225
410/547-2432 (fax)

ROBBINS GELLER RUDMAN
& DOWD LLP
STUART A. DAVIDSON
(*Pro Hac Vice* Pending)
sdavidson@rgrdlaw.com
CHRISTOPHER C. GOLD
(*Pro Hac Vice* Pending)
cgold@rgrdlaw.com
DOROTHY P. ANTULLIS
(*Pro Hac Vice* Pending)
dantullis@rgrdlaw.com
120 East Palmetto Park Road, Suite 500
Boca Raton, FL 33432
Telephone: 561/750-3000
561/750-3364 (fax)

MARK S. REICH
(*Pro Hac Vice* Pending)
mreich@rgrdlaw.com
58 South Service Road, Suite 200
Melville, NY 11747
Telephone: 631/367-7100
631/367-1173 (fax)

COHEN & MIZRAHI, LLP
DANIEL C. COHEN
(*Pro Hac Vice* Pending)
dan@cml.legal
EDWARD Y. KROUB
(*Pro Hac Vice* Pending)
edward@cml.legal
300 Cadman Plaza W., 12th Floor
Brooklyn, NY 11201
Telephone: 929/575-4175
929/575-4195 (fax)

Attorneys for Plaintiff and the Class